

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-208780

(43)Date of publication of application : 04.08.2005

(51)Int.Cl. G06F 13/00
H04L 12/58
H04L 12/66

(21)Application number : 2004-012542 (71)Applicant : NEC CORP

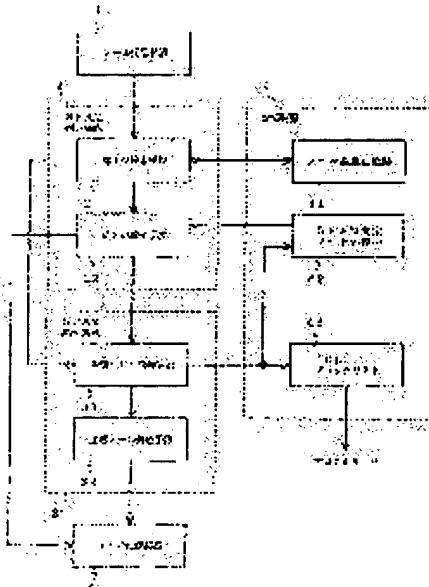
(22)Date of filing : 21.01.2004 (72)Inventor : YASUDA MASATO

(54) MAIL FILTERING SYSTEM AND URL BLACK LIST DYNAMIC CONSTRUCTION METHOD TO BE USED FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mail filtering device for reducing a management load by increasing the detection rate of an unsolicited bulk e-mail.

SOLUTION: A first retrieval means 21 retrieves the entry of a mail flow rate storage part 41 based on the transmission original IP address of the text of an electronic mail, and increases a corresponding count value by a specific value when the corresponding entry is found, and newly registers an entry constituted of the transmission original IP address of the electronic mail and the initial value of a counter in a mail flow rate storage part 41 when any corresponding entry is not found. A second retrieval means 22 retrieves whether or not the SPAM determination word of an SPAM determination word storage part 42 is included in the electronic mail. A new URL registering means 31 extracts a character string starting with "http" from the electronic mail, and records it in an SPAM determination word storage part 42 and a URL black list 43. An unsolicited bulk e-mail processing means 32 executes a preliminarily specified action to the unsolicited bulk e-mail.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-208780

(P2005-208780A)

(43) 公開日 平成17年8月4日(2005.8.4)

(51) Int. Cl. 7

G06F 13/00

H04L 12/58

H04L 12/66

F 1

G06F 13/00 610Q

H04L 12/58 100F

H04L 12/66 B

テーマコード(参考)

5K030

審査請求 未請求 請求項の数 31 O L (全 21 頁)

(21) 出願番号

特願2004-12542 (P2004-12542)

(22) 出願日

平成16年1月21日 (2004.1.21)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(74) 代理人 100088812

弁理士 ▲柳▼川 信

(72) 発明者 安田 真人

東京都港区芝五丁目7番1号 日本電気株式会社内

Fターム(参考) 5K030 GA15 HA08 HC01 HD03 HD06
JA10 KA05 MA13 MB18 MC08

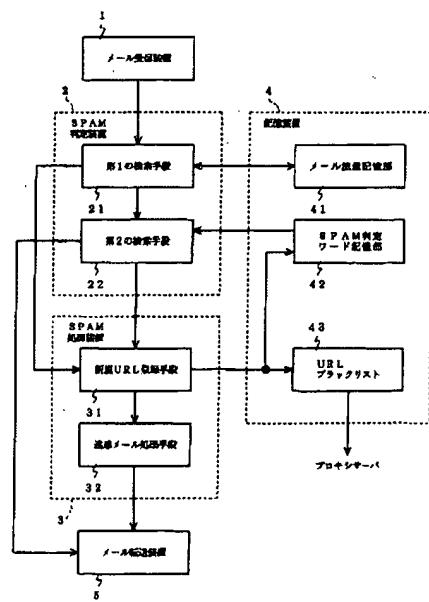
(54) 【発明の名称】メールフィルタリングシステム及びそれに用いるURLブラックリスト動的構築方法

(57) 【要約】

【課題】迷惑メールの検出率を高め、管理負担を軽減可能なメールフィルタリング装置を提供する。

【解決手段】第1の検索手段21は電子メールの本文の送信元IPアドレスを基にメール流量記憶部41のエントリを検索し、対応するエントリが見つかると対応するカウント値を規定値だけ増加させ、対応するエントリが見つからなければ電子メールの送信元IPアドレスとカウンタの初期値とからなるエントリをメール流量記憶部41に新規に登録する。第2の検索手段22は電子メールにSPAM判定ワード記憶部42のSPAM判定ワードが含まれていないかを検索する。新規URL登録手段31は電子メールから“http”で始まる文字列を抜き出し、SPAM判定ワード記憶部42及びURLブラックリスト43に記録する。迷惑メール処理手段32は迷惑メールに予め規定したアクションを実行する。

【選択図】 図1



【特許請求の範囲】**【請求項1】**

受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたURL (Uniform Resource Locator) を前記迷惑メールの判定ワード候補として登録する登録手段とを有し、その登録されたURLを基に前記検索手段が前記迷惑メールか否かを判定することを特徴とするメールフィルタリングシステム。

【請求項2】

一定時間のメールの流量をチェックするために前記電子メールのソースIP (Internet protocol) アドレスとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段とを含み、

前記検索手段は、前記受信メールのソースIPアドレスに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第1の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第2の検索手段とからなることを特徴とする請求項1記載のメールフィルタリングシステム。

【請求項3】

前記迷惑メールと判定された電子メールに対して少なくとも予め設定された廃棄及び遅延を行う迷惑メール処理手段を含むことを特徴とする請求項1または請求項2記載のメールフィルタリングシステム。

【請求項4】

前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたURLを記録するブラックリスト記録手段を含むことを特徴とする請求項1から請求項3のいずれか記載のメールフィルタリングシステム。

【請求項5】

前記登録手段は、前記迷惑メールと判定された電子メールの本文から取り出したURLが予め設定された所定URLの時に当該URLの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項4記載のメールフィルタリングシステム。

【請求項6】

前記ブラックリスト記録手段への記録を抑止するために予め設定された所定URLを記録するホワイトリスト記録手段を含むことを特徴とする請求項5記載のメールフィルタリングシステム。

【請求項7】

前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたURLを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項4から請求項6のいずれか記載のメールフィルタリングシステム。

【請求項8】

前記登録手段で取り出されたURLを一時保持するURL候補リスト記録手段を含み、前記URL候補リスト記録手段に保持されたURLを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項7記載のメールフィルタリングシステム。

【請求項9】

一定時間のメールの流量をチェックするために前記電子メールの本文から取り出されたURLとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段と、前記メール流量記憶手段のカウント値がしきい値を超えたエントリに対応する前記URLを取得する取得手段と、前記取得手段が取得したURLを記録するブラックリスト記録手段とを含み、

前記検索手段は、前記受信メールの本文から取り出されたURLに対応する前記メール

流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第1の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第2の検索手段とからなることを特徴とする請求項1記載のメールフィルタリングシステム。

【請求項10】

端末へ送信された電子メールのIP (Internet protocol) パケットから前記電子メールの本文を取り出すメール受信装置と、前記電子メールの流量をチェックするとともに迷惑メールと判定される用語が含まれていないかを検索しつつ前記迷惑メールと判定された電子メールの本文からURL (Uniform Resource Locator) を抽出して少なくとも廃棄及び遅延のうちの一方のアクションを起こすS P A M処理装置と、前記URLの文字列とカウント値との組み合わせをエントリとして記憶する記憶装置と、前記記憶装置に記憶されたURLとカウンタ値とからなるエントリの中の前記カウンタ値が予め設定されたしきい値を超えているものを取り出して前記記憶装置内のブラックリストに保存するブラックリスト構築装置と、前記電子メールの本文を前記IPパケットに収容して装置外に転送するメール転送装置とを有することを特徴とするメールフィルタリングシステム。

【請求項11】

受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたURL (Uniform Resource Locator) を前記迷惑メールの判定ワード候補として登録する登録手段とを有し、その登録されたURLを基に前記検索手段が前記迷惑メールか否かを判定することを特徴とするメールフィルタリング装置。

【請求項12】

一定時間のメールの流量をチェックするために前記電子メールのソースIP (Internet protocol) アドレスとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段とを含み、

前記検索手段は、前記受信メールのソースIPアドレスに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第一の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第二の検索手段とからなることを特徴とする請求項1記載のメールフィルタリング装置。

【請求項13】

前記迷惑メールと判定された電子メールに対して少なくとも予め設定された廃棄及び遅延を行う迷惑メール処理手段を含むことを特徴とする請求項11または請求項12記載のメールフィルタリング装置。

【請求項14】

前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたURLを記録するブラックリスト記録手段を含むことを特徴とする請求項11から請求項13のいずれか記載のメールフィルタリング装置。

【請求項15】

前記登録手段は、前記迷惑メールと判定された電子メールの本文から取り出したURLが予め設定された所定URLの時に当該URLの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項14記載のメールフィルタリング装置。

【請求項16】

前記ブラックリスト記録手段への記録を抑止するために予め設定された所定URLを記録するホワイトリスト記録手段を含むことを特徴とする請求項15記載のメールフィルタリング装置。

【請求項17】

前記迷惑メールと判定された電子メールの本文から前記登録手段で取り出されたURLを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記

録手段への記録を行うことを特徴とする請求項14から請求項16のいずれか記載のメールフィルタリング装置。

【請求項18】

前記登録手段で取り出されたURLを一時保持するURL候補リスト記録手段を含み、前記URL候補リスト記録手段に保持されたURLを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項17記載のメールフィルタリング装置。

【請求項19】

一定時間のメールの流量をチェックするために前記電子メールの本文から取り出されたURLとカウンタ値との組み合わせを保持するメール流量記憶手段と、予め設定された判定ワードを記憶する判定ワード記憶手段と、前記メール流量記憶手段のカウント値がしきい値を超えたエントリに対応する前記URLを取得する取得手段と、前記取得手段が取得したURLを記録するブラックリスト記録手段とを含み、

前記検索手段は、前記受信メールの本文から取り出されたURLに対応する前記メール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第一の検索手段と、前記判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第二の検索手段とからなることを特徴とする請求項11記載のメールフィルタリング装置。

【請求項20】

端末へ送信された電子メールのIP(Internet protocol)パケットから前記電子メールの本文を取り出すメール受信装置と、前記電子メールの流量をチェックするとともに迷惑メールと判定される用語が含まれていないかを検索しつつ前記迷惑メールと判定された電子メールの本文からURL(Uniform Resource Locator)を抽出して少なくとも廃棄及び遅延のうちの一方のアクションを起こすS-PAM処理装置と、前記URLの文字列とカウント値との組み合わせをエントリとして記憶する記憶装置と、前記記憶装置に記憶されたURLとカウンタ値とからなるエントリの中の前記カウンタ値が予め設定されたしきい値を超えているものを取り出して前記記憶装置内のブラックリストに保存するブラックリスト構築装置と、前記電子メールの本文を前記IPパケットに収容して装置外に転送するメール転送装置とを有することを特徴とするメールフィルタリング装置。

【請求項21】

受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてURL(Uniform Resource Locator)のブラックリストを構築するURLブラックリスト動的構築方法であって、

前記メールフィルタリング装置側に、前記受信メールが迷惑メールか否かを判定する第1のステップと、前記迷惑メールと判定された電子メールの本文に書かれたURLを前記迷惑メールの判定ワード候補として登録する第2のステップとを有し、

前記第1のステップは、その登録されたURLを基に前記迷惑メールか否かを判定することを特徴とするURLブラックリスト動的構築方法。

【請求項22】

前記第1のステップは、一定時間のメールの流量をチェックするために前記電子メールのソースIP(Internet protocol)アドレスとカウンタ値との組み合わせを保持するメール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第3のステップと、予め設定された判定ワードを記憶する判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第4のステップとを含むことを特徴とする請求項21記載のURLブラックリスト動的構築方法。

【請求項23】

前記メールフィルタリング装置側に、前記迷惑メールと判定された電子に対して少なくとも予め設定された廃棄及び遅延を行うステップを含むことを特徴とする請求項21また

は請求項22記載のURLブラックリスト動的構築方法。

【請求項24】

前記メールフィルタリング装置側に、前記迷惑メールと判定された電子メールの本文から前記第2のステップで取り出されたURLをブラックリスト記録手段に記録するステップを含むことを特徴とする請求項21から請求項23のいずれか記載のURLブラックリスト動的構築方法。

【請求項25】

前記第2のステップは、前記迷惑メールと判定された電子メールの本文から取り出したURLが予め設定された所定URLの時に当該URLの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項24記載のURLブラックリスト動的構築方法。

【請求項26】

前記第2のステップは、前記迷惑メールと判定された電子メールの本文から取り出したURLが前記ブラックリスト記録手段への記録を抑止するために予め設定された所定URLを記録するホワイトリスト記録手段に記録された所定URLの時に当該URLの前記ブラックリスト記録手段への記録を抑止することを特徴とする請求項25記載のURLブラックリスト動的構築方法。

【請求項27】

前記迷惑メールと判定された電子メールの本文から前記第2のステップで取り出されたURLを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項24から請求項26のいずれか記載のURLブラックリスト動的構築方法。

【請求項28】

前記第2のステップで取り出されたURLをURL候補リスト記録手段に一時保持し、前記URL候補リスト記録手段に保持されたURLを外部に表示し、その表示内容に基づいた外部からの指示に応じて前記ブラックリスト記録手段への記録を行うことを特徴とする請求項27記載のURLブラックリスト動的構築方法。

【請求項29】

前記第1のステップは、一定時間のメールの流量をチェックするために前記電子メールの本文から取り出されたURLとカウンタ値との組み合わせを保持するメール流量記憶手段のカウント値を規定値だけ増加させかつその値がしきい値を超えた時に前記迷惑メールと判定する第3のステップと、予め設定された判定ワードを記憶する判定ワード記憶手段に登録された前記判定ワードが前記受信メールの本文中に含まれている時に前記迷惑メールと判定する第4のステップとを含み、

前記メールフィルタリング装置側に、前記メール流量記憶手段のカウント値がしきい値を超えたエントリに対応する前記URLを取得するステップと、その取得したURLをブラックリスト記録手段に記録するステップとを含むことを特徴とする請求項21記載のURLブラックリスト動的構築方法。

【請求項30】

端末へ送信された電子メールのIP(Internet protocol)パケットから前記電子メールの本文をメール受信装置にて取り出し、前記電子メールの流量をチェックするとともに迷惑メールと判定される用語が含まれていないかを検索しかつ前記迷惑メールと判定された電子メールの本文からURL(Uniform Resource Locator)を抽出して少なくとも廃棄及び遅延のうちの一方のアクションをSMA(M)処理装置にて実行し、前記URLの文字列とカウント値との組み合わせをエントリとして記憶装置に記憶し、前記記憶装置に記憶されたURLとカウンタ値とからなるエントリの中の前記カウンタ値が予め設定されたしきい値を超えているものをブラックリスト構築装置にて取り出して前記記憶装置内のブラックリストに保存し、メール転送装置にて前記電子メールの本文を前記IPパケットに収容して装置外に転送することを特徴とするURLブラックリスト動的構築方法。

【請求項31】

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-208780

(P2005-208780A)

(43) 公開日 平成17年8月4日(2005.8.4)

(51) Int. Cl. 7

G06F 13/00
H04L 12/58
H04L 12/66

F 1

G06F 13/00
H04L 12/58
H04L 12/66

テーマコード(参考)

5K030

審査請求 未請求 請求項の数 31 O L (全 21 頁)

(21) 出願番号
(22) 出願日特願2004-12542 (P2004-12542)
平成16年1月21日 (2004.1.21)(71) 出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号
(74) 代理人 100088812
弁理士 ▲柳▼川 信
(72) 発明者 安田 真人
東京都港区芝五丁目7番1号 日本電気株式会社内
F ターム(参考) 5K030 GA15 HA08 HC01 HD03 HD06
JA10 KA05 MA13 MB18 MC08

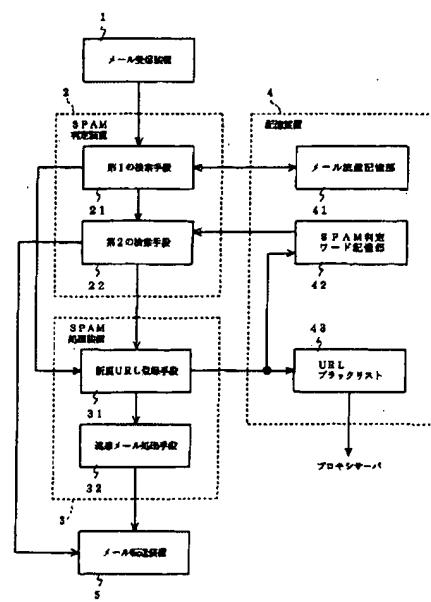
(54) 【発明の名称】メールフィルタリングシステム及びそれに用いるURLブラックリスト動的構築方法

(57) 【要約】

【課題】迷惑メールの検出率を高め、管理負担を軽減可能なメールフィルタリング装置を提供する。

【解決手段】第1の検索手段21は電子メールの本文の送信元IPアドレスを基にメール流量記憶部41のエントリを検索し、対応するエントリが見つかると対応するカウント値を規定値だけ増加させ、対応するエントリが見つからなければ電子メールの送信元IPアドレスとカウンタの初期値からなるエントリをメール流量記憶部41に新規に登録する。第2の検索手段22は電子メールにSPAM判定ワード記憶部42のSPAM判定ワードが含まれていないかを検索する。新規URL登録手段31は電子メールから“http”で始まる文字列を抜き出し、SPAM判定ワード記憶部42及びURLブラックリスト43に記録する。迷惑メール処理手段32は迷惑メールに予め規定したアクションを実行する。

【選択図】 図1



受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてURL (Uniform Resource Locator) のブラックリストを構築するURLブラックリスト動的構築方法のプログラムであって、コンピュータに、前記受信メールが迷惑メールか否かを判定する第1の処理と、前記迷惑メールと判定された電子メールの本文に書かれたURLを前記迷惑メールの判定ワード候補として登録する第2の処理とを実行させ、前記第1の処理においてその登録されたURLを基に前記迷惑メール【発明の詳細な説明】るためのプログラム。

【技術分野】

【0001】

本発明はメールフィルタリングシステム、メールフィルタリング装置及びそれらに用いるURLブラックリスト動的構築方法並びにそのプログラムに関し、特に迷惑メール等をフィルタリングするメールフィルタリングシステムに関する。

【背景技術】

【0002】

メールフィルタリングシステムは、広告業者が大量のメールアドレスに対して送信した迷惑メールをユーザに届く前に遮断したり、遅延させることによって、ユーザのSPAMメールによる被害及びネットワーク内に掛かる負荷を低減させるために用いられている。

【0003】

従来、メールフィルタリング装置の一例としては、SPAM判定ワードが電子メールの本文中に含まれていた場合、その電子メールを拒否する装置がある。このメールフィルタリング装置は、主にネットワークインターフェース部（IF部）と、メール記憶部と、不要メール情報管理部と、メール受信制御部と、WEBメール装置とから構成されている（例えば、特許文献1参照）。

【0004】

ネットワークインターフェース部は、ネットワークとの情報・データの授受を制御し、送信者端末からの電子メールを受信する。メール記憶部はインターフェース部で受信する電子メールを保管する。不要メール情報管理部はメール送信元の識別情報等、不要メールや迷惑メールに関する各種情報を記憶する。

【0005】

WEBメール装置は受信者端末にてに送られてきた電子メールの各種情報を表示されるWEB上の所定領域である。メール受信制御部はネットワークインターフェース部とメール記憶部と不要メール情報管理部とWEBメール装置とを制御し、不要メールや迷惑メールのフィルタリング設定等を行う。

【0006】

上記のメールフィルタリング装置では、受信した電子メールをメール記憶部に記憶し、その電子メールを不要メール情報管理部の記憶内容と比較し、一致した場合に迷惑メールとみなし、その電子メールの受信を拒否している。

【0007】

【特許文献1】特開2003-173314号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、上述した従来のメールフィルタリング装置では、不要メール情報管理部にSPAM判定ワードのリストのみが記入されており、一定時間のメールの流量をチェックしていないので、不要メール情報管理部に記憶したSPAM判定ワードがメール本文中に記載されていない限り、ネットワークの負荷が増大してしまうような迷惑メールも全て通過してしまうという問題がある。

【0009】

また、従来のメールフィルタリング装置では、迷惑メールを検知した時に、迷惑メールを拒否するだけで、当該迷惑メールの内容を不要メール情報管理部のデータベースにフィ

ードバックしていないので、SPAM判定ワードを手作業で登録しなければならないという問題がある。

【0010】

さらに、従来のメールフィルタリング装置では、迷惑メールを検知した時に、迷惑メールを拒否するだけで、当該迷惑メールの内容を不要メール情報管理部のデータベースにフィードバックしていないので、迷惑メールを見つけた場合、迷惑メールを拒否するだけなので、同一広告業者が電子メールの本文の内容を変えて迷惑メールを送信すると、それに対処することができないという問題がある。

【0011】

そこで、本発明の目的は上記の問題点を解消し、迷惑メールの検出率を高めることができ、管理負担を軽減することができるメールフィルタリングシステム、メールフィルタリング装置及びそれらに用いるURLブラックリスト動的構築方法並びにそのプログラムを提供することにある。

【課題を解決するための手段】

【0012】

本発明によるメールフィルタリングシステムは、受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたURL (Uniform Resource Locator) を前記迷惑メールの判定ワード候補として登録する登録手段とを備え、その登録されたURLを基に前記検索手段が前記迷惑メールか否かを判定している。

【0013】

本発明によるメールフィルタリング装置は、受信メールが迷惑メールか否かを判定する検索手段と、前記迷惑メールと判定された電子メールの本文に書かれたURL (Uniform Resource Locator) を前記迷惑メールの判定ワード候補として登録する登録手段とを備え、その登録されたURLを基に前記検索手段が前記迷惑メールか否かを判定している。

【0014】

本発明によるURLブラックリスト動的構築方法は、受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてURL (Uniform Resource Locator) のブラックリストを構築するURLブラックリスト動的構築方法であって、

前記メールフィルタリング装置側に、前記受信メールが迷惑メールか否かを判定する第1のステップと、前記迷惑メールと判定された電子メールの本文に書かれたURLを前記迷惑メールの判定ワード候補として登録する第2のステップとを備え、

前記第1のステップは、その登録されたURLを基に前記迷惑メールか否かを判定している。

【0015】

本発明によるURLブラックリスト動的構築方法のプログラムは、受信メールのフィルタリング処理を行うメールフィルタリング装置を含むシステムにおいてURL (Uniform Resource Locator) のブラックリストを構築するURLブラックリスト動的構築方法のプログラムであって、コンピュータに、前記受信メールが迷惑メールか否かを判定する第1の処理と、前記迷惑メールと判定された電子メールの本文に書かれたURLを前記迷惑メールの判定ワード候補として登録する第2の処理とを実行させ、前記第1の処理においてその登録されたURLを基に前記迷惑メールか否かを判定させている。

【0016】

すなわち、本発明のメールフィルタリングシステムは、迷惑メール (SPAMメール) の本文に書かれたURL (Uniform Resource Locator) をSPAM判定ワードの候補として登録し、同じ広告業者から来たメールをフィルタリング可能にすることを特徴としている。

【0017】

また、本発明のメールフィルタリングシステムは、迷惑メールと判定した後、迷惑メールの本文に書かれたURLを新規にデータベースに登録し、広告業者のURLブラックリストの候補を自動生成することを特徴としている。

【0018】

より具体的に説明すると、本発明のメールフィルタリングシステムでは、SPAM判定装置がメール受信装置から電子メールのパケット情報を受け取り、第一の検索手段及び第二の検索手段の2カ所で迷惑メールかどうかの判定を行っている。

【0019】

第一の検索手段ではメール流量記憶部内の受信メールのソースIP(Internet Protocol)アドレスに対応するエントリのカウント値を規定値だけ増加させ、その値がしきい値を超えた場合、迷惑メールと判定する。

【0020】

第二の検索手段ではSPAM判定ワード記憶部に記憶されたSPAM判定ワードが電子メールの本文中に含まれていないかを検索し、SPAM判定ワードが含まれていた場合に迷惑メールと判定する。

【0021】

SPAM判定ワード記憶部には、予め設定したSPAM判定ワードリストが記録されている。SPAM判定ワードとは、電子メールの本文中に含まれていたら迷惑メールと判定される“出会い系”、“アダルト”等の言葉である。

【0022】

迷惑メールとみなされたメールは、新規URL登録手段によって、電子メール本文から“http(hyper text transfer protocol)”から始まる文字列がURLとして取り出され、取り出したURLがSPAM判定ワード記憶部とURLブラックリストとに登録されていない場合、新規にSPAM判定ワード記憶部とURLブラックリストとに登録する。

【0023】

URL登録後、迷惑メール処理手段は、電子メールに対してユーザが設定したアクション(電子メールの廃棄や電子メールの遅延等)が行われる。装置外に電子メールが転送されるアクションの場合には、メール送信装置によって電子メールの本文が送られる。

【0024】

これによって、本発明のメールフィルタリングシステムでは、迷惑メールを発送した広告業者のURLブラックリストを動的に構築することが可能となる。つまり、本発明のメールフィルタリングシステムでは、携帯電話機等に送られるSPAMメールの文字数が少ない代わりに、広告サイトのURLリンクがメール本文中にほぼ必ず貼られるという点に着目し、SPAMメール内にあったURLリンクをSPAM判定ワードとして登録することによって、SPAMメールの検出率を高めることが可能となる。

【0025】

また、本発明のメールフィルタリングシステムでは、迷惑メールからURLを取得して自動的にURLブラックリストを生成しているので、迷惑メールに記載されたURLへのアクセスを禁止するために、管理者がブラックリストのURLを自ら収集して手作業で登録する必要がなくなり、管理負担を軽減することが可能となる。

【0026】

迷惑メールからURLを抽出する理由は、迷惑メールの多くが広告用サイトの宣伝に用いられ、電子メールの本文の中には必ず広告用サイトのURLリンクが貼られているので、その抽出したURLから迷惑メールを特定することが可能となるからである。

【0027】

しかしながら、実用の際には、取得したURLを、ブラックリストに登録しても良いかどうかをチェックする必要がある。その際、取得したURLをSPAM判定ワード記憶部及びURLブラックリストに登録する前に、一旦、別に用意したURL候補リストに保存

し、オペレータがその候補リストの中から登録しても良いものを選び出すことによって登録されるようにするとよい。

【0028】

さらに、本発明のメールフィルタリングシステムでは、迷惑メールから抽出したURLをSPAM判定ワード記憶部に登録することによって、一度、迷惑メールを配布した広告主と同じ広告主から送信元を変えてその迷惑メールが配布される場合でも、同じ広告主からの電子メールを全て迷惑メールとして処理することが可能となる。

【0029】

SPAM判定ワード記憶部に登録して迷惑メールのチェックをする理由として、時間T0から迷惑メールが大量に送信されたとすると、時間T0から時間T1にかけてメール流量記憶部で流量がカウントされ、時間T1で閾値を超えるとすると、時間T1以降の迷惑メールが迷惑メールとして認識される。逆に言えば、時間T0から時間T1にかけての電子メールは迷惑メールとして処理されない。

【0030】

続いて、時間T2から充分に時間が経過した時間T3に、同じ広告業者の迷惑メールが大量に流れてきたとすると、時間T3から時間T4にかけての電子メールは、もし迷惑メールから抽出したURLをSPAM判定ワード記憶部に記憶していなければ、メール流量記憶部のカウント値がリセットされる程、充分に時間が経過しているために、カウントが閾値を超えるまでは迷惑メールが通過してしまうが、迷惑メールから抽出したURLをSPAM判定ワード記憶部に記憶していれば、第一の検索手段で迷惑メールとして検出されなかった迷惑メールも、第二の検索手段で迷惑メールとして認識されるので、一度、迷惑メールとして認識した電子メールを再び通過させてしまうことがなくなる。

【0031】

さらにまた、本発明のメールフィルタリングシステムでは、迷惑メールからURLを抽出して直接ブラックリストを生成しているので、局所的にしか出回らない広告メールのURLもブラックリストに登録することが可能となる。

【0032】

本発明のメールフィルタリングシステムでは、電子メールの本文の内容が変わっても、同一広告業者のサイトとして同じURLが迷惑メールの本文中に含まれていることを利用し、URLを不要メール情報管理部のデータベースにフィードバックしているので、同一広告業者が電子メールの本文の内容を変えて迷惑メールを送信しても、あるいは送信元を変えて迷惑メールを送信しても、それらに対処することが可能となる。

【発明の効果】

【0033】

本発明は、以下に述べるような構成及び動作とすることで、迷惑メールの検出率を高めることができ、管理者の管理負担を軽減することができるという効果が得られる。

【発明を実施するための最良の形態】

【0034】

次に、本発明の実施例について図面を参照して説明する。図1は本発明の一実施例によるメールフィルタリング装置（システム）の構成を示すブロック図である。図1において、本発明の一実施例によるメールフィルタリング装置は、携帯電話やメール端末等へ送信された電子メールのIP(Internet Protocol)パケットから電子メールの本文を取り出すメール受信装置1と、電子メールの流量をチェックするとともに迷惑(SPAM)メールと判定される用語が含まれていないかを検索するSPAM判定装置2と、迷惑メールと判定された電子メールの本文からURL(Uniform Resource Locator)を抽出して廃棄・遅延等のアクションを起こすSPAM処理装置3と、情報を記憶する記憶装置4と、電子メールの本文をIPパケットに収容して装置外に転送するメール転送装置5とから構成されている。

【0035】

これらメール受信装置1、SPAM判定装置2、SPAM処理装置3、記憶装置4、メ

ール転送装置5は、それぞれプログラム制御によって動作する。ここで言うプログラムは、FPGA (Field Programmable Gate Array) 等の論理回路を含む。

【0036】

メール受信装置1はパケットから電子メールの送信元IPアドレス情報と電子メールの本文とを文字列として取り出し、その文字列をSPAM判定装置2に出力する。

【0037】

SPAM判定装置2は第1の検索手段21と、第2の検索手段22とを備えている。第1の検索手段21はメール受信装置1から与えられた電子メールの本文の送信元IPアドレスをキーとしてメール流量記憶部41に記憶されたエントリを検索する。

【0038】

第1の検索手段21は対応するエントリが見つかった場合、対応するカウント値を規定値だけ増加させる。また、第1の検索手段21は対応するエントリが存在しない場合、メールの送信元IPアドレスとカウンタの初期値とからなるエントリをメール流量記憶部41に新規に登録する。

【0039】

第2の検索手段22はSPAM判定ワード記憶部42からSPAM判定ワードのリストを取得し、電子メールの本文中にSPAM判定ワードが含まれていないかを検索する。

【0040】

SPAMメール処理装置3は新規URL登録手段31と、迷惑メール処理手段32とを備えている。新規URL登録手段31は電子メールの本文中から“http (hyper text transfer protocol)”で始まる文字列を抜き出し、SPAM判定ワード記憶部42及びURLブラックリスト43に記録する。

【0041】

迷惑メール処理手段32は予め規定したアクションを受信した迷惑メールに対して実行する。例えば、迷惑メール処理手段32は規定されたアクションが廃棄であれば、メール転送装置5に受信メールを渡さずに、電子メールの情報を解放する。また、迷惑メール処理手段32は規定されたアクションが遅延であれば、メール転送装置5に受信メールを渡す時間を遅らせる。

【0042】

記憶装置4はメール流量記憶部41と、SPAM判定ワード記憶部42と、URLブラックリスト43とを備えている。メール流量記憶部41は一定時間のメールの流量をチェックするために検索テーブル形式をとり、検索キーとしてソースIPアドレス、対応データとしてカウンタ値をとる。このカウンタ値は一定時間毎に値が減算され、カウンタ値が「0」になると、対応するエントリが削除される。

【0043】

SPAM判定ワード記憶部42はSPAMメールの判定基準となる言葉がリスト形式で記録されている。このリストはオペレータによって予め登録された項目と、新規URL登録手段31から登録された項目とからなる。URLブラックリスト43は新規URL登録手段31によって取り出されたURLを記録しており、その記憶内容は図示せぬプロキシサーバ等から読み出し可能となっている。

【0044】

プロキシサーバでは、上記のURLブラックリスト43から読み出した記憶内容を基に、迷惑メールと判定された電子メールから取り出したURLへのアクセスを禁止する制御を行う。したがって、本実施例では、プロキシサーバの代わりに、上記のURLへのアクセスを禁止する手段であれば、インターネットへのアクセス制御手段を配置することも可能である。

【0045】

メール転送装置5は上記の第2の検索手段22または迷惑メール処理手段32から渡された電子メールの本文を、IPパケットとして送信先に転送する。このメール転送装置5

としてはメールサーバ等が考えられ、その転送先としては電子メールの送受信を行う端末等が考えられる。

【0046】

尚、この端末としては携帯電話端末も考えられる。その場合、携帯電話端末にはS P A M判定装置2とS P A M処理装置3と記憶装置4とが搭載され、URLブラックリスト43の記憶内容がアクセス制御手段に渡されることで、迷惑メールに記載されたURLへのアクセスをアクセス制御手段によって制限することが可能となる。

【0047】

図2及び図3は本発明の一実施例によるメールフィルタリング装置の動作を示すフローチャートである。これら図1～図3を参照して本発明の一実施例によるメールフィルタリング装置の動作について説明する。

【0048】

メール受信装置1は電子メールの入ったIPパケットを受信すると、その電子メールのIPパケットから送信元のIPアドレスを含むパケット情報と電子メールの本文とを含むメール情報を取得し、第1の検索手段21に供給する(図2ステップS1)。

【0049】

第1の検索手段21はメール受信装置1から受け取ったパケット情報のソースIPアドレスと同じソースIPアドレスがメール流量記憶部41に記載されているかどうかを調べる(図2ステップS2)。

【0050】

第1の検索手段21はメール流量記憶部41に同じソースIPアドレスが記憶されている場合(図2ステップS3)、対応するカウンタ値を読み出し、そのカウンタ値を規定値だけ増加させる(図2ステップS4)。その結果、カウンタ値が予め設定したしきい値を超えた場合(図2ステップS5)、第1の検索手段21はそのIPアドレスに対応したメールを迷惑メールとみなし、電子メールの本文をS P A Mメール処理装置3に送る。超えなかった場合(図2ステップS5)、第1の検索手段21はその電子メールの本文を第2の検索手段22に送る。

【0051】

第1の検索手段21は同じソースIPアドレスがメール流量記憶部41に記憶されていなかった場合(図2ステップS3)、ソースIPアドレスとカウンタの初期値とからなるエントリをメール流量記憶部41に記録する(図2ステップS6)。

【0052】

メール流量記憶部41ではソースIPアドレスとカウンタ値との組み合わせからなるエントリが登録されており、一定時間が経過する毎に全エントリのカウンタ値が規定値だけ減少し、カウンタ値が「0」以下になると、そのエントリが削除される。

【0053】

第2の検索手段22は第1の検索手段21から受け取った電子メールの本文にS P A M判定ワードが含まれていないかどうかを検索する(図2ステップS7)。第2の検索手段22は検索するS P A M判定ワードをS P A M判定ワード記憶部41から取得する。

【0054】

電子メールの本文にS P A M判定ワードが含まれていない場合(図2ステップS8)、第2の検索手段22はメール情報をメール転送装置5に送る。S P A M判定ワードが含まれていた場合(図2ステップS8)、第2の検索手段22はメール情報をS P A Mメール処理装置3に送る。

【0055】

S P A Mメール処理装置3に送られたメール情報は、最初に新規URL登録手段31で処理される。新規URL登録手段31は電子メールの本文中から“h t t p”で始まるURLを文字列として取り出す(図3ステップS9)。

【0056】

URLの取得に成功した場合(図3ステップS10)、新規URL登録手段31は取得

したURLをSPAM判定ワード記憶部42及びURLブラックリスト43に記憶し、迷惑メール処理手段32に処理を移す(図3ステップS11, S12)。

【0057】

URLの取得に失敗した場合(図3ステップS10)、新規URL登録手段31はURLの登録処理なしとし、処理を迷惑メール処理手段32に移す。迷惑メール処理手段32は新規URL登録手段31から受け取った電子メールに対して予め規定したアクションを実行する(図3ステップS13)。

【0058】

規定したアクションの例としては、通過や廃棄、そして遅延がある。通過の場合には、メール情報をそのままメール転送装置5に転送する。廃棄の場合には、メール情報を迷惑メール処理手段32で止め、全て解放する。遅延の場合には、迷惑メール処理手段32で遅延されてメール転送装置5に送られる。

【0059】

メール転送装置5は迷惑メール処理手段32もしくは第2の検索手段22から送られてきたメール情報をIPパケットの形式に変換し、電子メールの送信先へと転送する(図3ステップS14)。

【0060】

このように、本実施例では、携帯電話機等に送られる迷惑メールが、文字数が少ない代わりに、広告サイトのURLリンクが電子メールの本文中にほぼ必ず貼られるという点に着目し、迷惑メール内にあったURLリンクをSPAM判定ワードとして登録することによって、SPAMメールの検出率を高めることができる。

【0061】

また、本実施例では、迷惑メールからURLを取得して自動的にURLブラックリストを生成しているので、管理者がブラックリストのURLを自ら収集して手作業で登録する必要がなくなり、管理負担を軽減することができる。迷惑メールからURLを抽出する理由としては、迷惑メールの多くが広告用サイトの宣伝に用いられ、電子メールの本文中にほぼ必ず広告用サイトのURLリンクが貼られているので、そのURLから迷惑メールを特定することができるためである。

【0062】

しかしながら、実用の際には、取得したURLにブラックリストに登録されても良いかどうかをチェックする必要がある。その際、後述するように、取得したURLをSPAM判定ワード記憶部42及びURLブラックリスト43に登録する前に、一旦、別に用意したURL候補リストに保存し、オペレータがその候補リストの中から登録しても良いものを選び出すことによって登録されることによるとよい。

【0063】

さらに、本実施例では、迷惑メールから抽出したURLをSPAM判定ワード記憶部42に登録することによって、一度、迷惑メールを配布した広告主と同じ広告主からのメールを全て迷惑メールとして処理することができる。

【0064】

図4を参照してSPAM判定ワード記憶部42にURLを登録して迷惑メールのチェックを行う理由について説明する。図4に示すように、時間T0から迷惑メールが大量に送信されたとすると、時間T0から時間T1にかけての時間帯A1に、メール流量記憶部41で流量がカウントされ、時間T1で閾値を超えるとすると、時間T1以後の時間帯A2の迷惑メールが迷惑メールとして認識される。逆に言えば、時間T0から時間T1にかけて時間帯A1の電子メールは、迷惑メールとして処理されない。

【0065】

続いて、時間T2から充分に時間が経過した時間T3に、同じ広告業者の迷惑メールが大量に流れてきたとすると、時間T3から時間T4にかけての時間帯A3の電子メールは、もし迷惑メールから抽出したURLをSPAM判定ワード記憶部42に記憶させていなければ、メール流量記憶部41のカウント値がリセットされる程、充分に時間が経過して

いるために、カウントが閾値を超えるまでは迷惑メールが通過してしまう。但し、時間T4で閾値を超えると、時間T4以降の時間帯A4の迷惑メールが迷惑メールとして認識される。

【0066】

しかしながら、迷惑メールから抽出したURLをSPAM判定ワード記憶部42に記憶していれば、第1の検索手段21で迷惑メールとして検出されなかった迷惑メールも、第2の検索手段22で迷惑メールとして認識されるので、一度、時間帯A2で迷惑メールとして認識した電子メールを、時間帯A3において再び通過させてしまうことがなくなる。

【0067】

さらにまた、本実施例では、迷惑メールからURLを抽出して直接ブラックリストを生成しているので、局所的にしか出回らない広告メールのURLもブラックリストに登録することができる。

【0068】

図5は本発明の他の実施例によるメールフィルタリング装置の構成を示すブロック図である。図5において、本発明の他の実施例によるメールフィルタリング装置は記憶装置6にURLホワイトリスト61を追加した以外は図1に示す本発明の一実施例と同様の構成となっており、同一構成要素には同一符号を付してある。本実施例において、URLホワイトリスト61にはURLブラックリスト43に登録させたくないURLが予め登録されている。

【0069】

例えば、短時間に大量に送信されるメールとしては、必ずしも迷惑メールだけではなく、メールマガジン等がある。このメールマガジン等では同一IPアドレスから大量にメールが送信されるので、メール流量のしきい値を超えて迷惑メールとみなされることがある。

【0070】

このメールマガジン等のURLはURLホワイトリスト61にURLブラックリスト43に登録させたくないURLとして登録しておくことで、上記の不具合を解消することができる。

【0071】

図6及び図7は本発明の他の実施例によるメールフィルタリング装置の動作を示すフローチャートである。これら図5～図7を参照して本発明の他の実施例によるメールフィルタリング装置の動作について説明する。図6のステップS21～S28及び図7のステップS29、S32～S35は図2のステップS1～S8及び図3のステップS9、S11～S14と同様の動作であるので、その動作についての説明は省略する。

【0072】

メールコンテンツからURLを抽出した後(図7ステップS29)、新規URL登録手段31は抽出したURLをキーとしてURLホワイトリスト61を検索する(図7ステップS30)。新規URL登録手段31は検索に成功すれば(図7ステップS31)、迷惑メール処理を行わず、メール転送装置5に渡してその電子メールを転送する(図7ステップS35)。

【0073】

新規URL登録手段31は検索に失敗した場合(図7ステップS31)、SPAM判定ワード記憶部42とURLブラックリスト43とにそれぞれエントリを追加し(図7ステップS32、S33)、迷惑メール処理手段32にて迷惑メール処理を行う(図7ステップS34)。

【0074】

尚、URLホワイトリスト61ではホワイトリストのエントリをURLとしているが、ホワイトリストのエントリをURLではなく、送信元メールアドレスとして登録してもよい。この場合、メールマガジンの本文にURLが含まれていなくても迷惑メールとしてフィルタリングされることはない。

【0075】

図8は本発明の別の実施例によるメールフィルタリング装置の構成を示すブロック図である。図8において、本発明の別の実施例によるメールフィルタリング装置は記憶装置7に登録候補リスト71を追加し、登録候補リスト71に登録許可を指示するオペレータ制御部8を設けた以外は図1に示す本発明の一実施例と同様の構成となっており、同一構成要素には同一符号を付してある。

【0076】

迷惑メールの本文から取得したURLは、必ずしも広告業者のURLのみが含まれているとは限らない。そのため、取得したURLをURLブラックリスト43に登録すべきか否かの判断をする必要がある。

【0077】

そこで、本実施例では記憶装置7内に新たに登録候補リスト71を設置し、新規URL登録手段31によって取得したURLを一時的に登録候補リスト71に記憶する。

【0078】

オペレータはオペレータ制御部8から登録候補リスト71に記憶されているURLのリストを参照し、登録の許可・不許可を決定し、登録を許可されたURLのみSPAM判定ワード記憶部42及びURLブラックリスト43に記憶させるようにする。これによって、本実施例では、本来、URLブラックリスト43に載せるべきではないURLを事前に排除することができる。

【0079】

図9は本発明の別の実施例によるメールフィルタリング装置の動作を示すフローチャートであり、図10は本発明の別の実施例によるオペレータ制御部8における登録候補リスト選択処理を示すフローチャートである。これら図8～図10を参照して本発明の別の実施例によるメールフィルタリング装置の動作について説明する。

【0080】

メール受信装置1は電子メールの入ったIPパケットを受信すると、その電子メールのIPパケットから送信元のIPアドレスを含むパケット情報と電子メールの本文とを含むメール情報を取得し、第1の検索手段21に供給する(図9ステップS61)。

【0081】

第1の検索手段21はメール受信装置1から受け取ったパケット情報のソースIPアドレスと同じソースIPアドレスがメール流量記憶部41に記載されているかどうかを調べる(図9ステップS62)。

【0082】

第1の検索手段21はメール流量記憶部41に同じソースIPアドレスが記憶されている場合(図9ステップS63)、対応するカウンタ値を読み出し、そのカウンタ値を規定値だけ増加させる(図9ステップS64)。その結果、カウンタ値が予め設定したしきい値を超えた場合(図9ステップS65)、第1の検索手段21はそのIPアドレスに対応したメールを迷惑メールとみなし、電子メールの本文をSPAMメール処理装置3に送る。超えなかった場合(図9ステップS65)、第1の検索手段21はその電子メールの本文を第2の検索手段22に送る。

【0083】

第1の検索手段21は同じソースIPアドレスがメール流量記憶部41に記憶されていなかった場合(図9ステップS63)、ソースIPアドレスとカウンタの初期値とからなるエントリをメール流量記憶部41に記録する(図9ステップS66)。

【0084】

メール流量記憶部41ではソースIPアドレスとカウンタ値との組み合わせからなるエントリが登録されており、一定時間が経過する毎に全エントリのカウンタ値が規定値だけ減少し、カウンタ値が「0」以下になると、そのエントリが削除される。

【0085】

第2の検索手段22は第1の検索手段21から受け取った電子メールの本文にSPAM

判定ワードが含まれていないかどうかを検索する(図9ステップS67)。第2の検索手段22は検索するSPAM判定ワードをSPAM判定ワード記憶部41から取得する。

【0086】

電子メールの本文にSPAM判定ワードが含まれていない場合(図9ステップS68)、第2の検索手段22はメール情報をメール転送装置5に送る。SPAM判定ワードが含まれていた場合(図9ステップS68)、第2の検索手段22はメール情報をSPAMメール処理装置3に送る。

【0087】

SPAMメール処理装置3に送られたメール情報は、最初に新規URL登録手段31で処理される。新規URL登録手段31は電子メールの本文中から“http”で始まるURLを文字列として取り出す(図9ステップS69)。

【0088】

URLの取得に成功した場合(図9ステップS70)、新規URL登録手段31は取得したURLを登録候補リスト71に記憶し、迷惑メール処理手段32に処理を移す(図9ステップS71, S72)。

【0089】

URLの取得に失敗した場合(図9ステップS70)、新規URL登録手段31はURLの登録処理なしとし、処理を迷惑メール処理手段32に移す。迷惑メール処理手段32は新規URL登録手段31から受け取った電子メールに対して予め規定したアクションを実行する(図9ステップS73)。

【0090】

規定したアクションの例としては、通過や廃棄、そして遅延がある。通過の場合には、メール情報をそのままメール転送装置5に転送する。廃棄の場合には、メール情報を迷惑メール処理手段32で止め、全て解放する。遅延の場合には、迷惑メール処理手段32で遅延されてメール転送装置5に送られる。

【0091】

メール転送装置5は迷惑メール処理手段32もしくは第2の検索手段22から送られてきたメール情報をIPパケットの形式に変換し、電子メールの送信先へと転送する(図9ステップS74)。

【0092】

次に、オペレータが登録候補リスト71に登録されたURLの中からURLを選択してSPAM判定ワード記憶部42やURLブラックリスト43に登録する処理について説明する。

【0093】

この場合、オペレータ制御部8はオペレータから指示があると、メールフィルタリング装置にログインし(図10ステップS81)、登録候補リスト71に登録されたURLをダウンロードして表示する(図10ステップS82)。

【0094】

オペレータ制御部8はオペレータが表示されたURLの中から登録URLを選択すると(図10ステップS83)、その登録URLをSPAM判定ワード記憶部42及びURLブラックリスト43に追加登録し(図10ステップS84)、メールフィルタリング装置からログアウトする(図10ステップS85)。

【0095】

このように、本実施例では、オペレータがオペレータ制御部8から登録候補リスト71に記憶されているURLのリストを参照し、登録の許可・不許可を決定し、登録を許可されたURLのみSPAM判定ワード記憶部42及びURLブラックリスト43に記憶させることで、本来、URLブラックリスト43に載せるべきではないURLを事前に排除することができる。

【0096】

図11は本発明のさらに別の実施例によるメールフィルタリング装置の構成を示すプロ

ック図である。図11において、本発明のさらに別の実施例によるメールフィルタリング装置は携帯電話やメール端末等へ送信された電子メールのIPパケットから電子メールの本文を取り出すメール受信装置1と、電子メールの流量をチェックするとともに迷惑(SPAM)メールと判定される用語が含まれていないかを検索し、迷惑メールと判定された電子メールの本文からURLを抽出して廃棄・遅延等のアクションを起こすSPAM処理装置9と、情報を記憶する記憶装置10と、ブラックリスト構築装置11と、電子メールの本文をIPパケットに収容して装置外に転送するメール転送装置5とから構成されている。

【0097】

本実施例は、迷惑メールの判定後に行っていた電子メールの本文からのURL取得をメール受信の次に行わせることにした点で、上述した本発明の一実施例によるメールフィルタリング装置と異なっている。

【0098】

また、本実施例では、装置構成を、図1に示すSPAM判定装置2及びSPAM処理装置3をSPAM処理装置9に統合し、図1の記憶装置4のURLブラックリスト43をブラックリスト構築装置11のURLブラックリスト記憶部112に分割させた点で、上述した本発明の一実施例によるメールフィルタリング装置と異なっている。

【0099】

SPAM処理装置9はURL取得手段91と、第1の検索手段92と、第2の検索手段93と、迷惑メール処理手段94とを備えている。URL取得手段91はメール受信装置1から受け取った電子メールの本文の文面から“http”で始まる文字列をURLとして取得する。第1の検索手段92は取得されたURLをキーとして、メール流量記憶部101に記憶されたURLを検索する。

【0100】

記憶装置10のメール流量記憶部101は、図1のメール流量記憶部41がソースIPアドレスとカウント値との組み合わせがエントリとして記憶しているのに対し、URLの文字列とカウント値との組み合わせをエントリとして記憶している点で、上述した本発明の一実施例によるメールフィルタリング装置と異なっている。カウント値は一定時間経過すると規定値だけ減少し、カウント値が「0」以下になると対応したエントリが削除される。

【0101】

ブラックリスト構築装置11はブラックリスト抽出手段111と、URLブラックリスト記憶部112とを備えている。ブラックリスト抽出手段111はメール流量記憶部101に記憶されたURLとカウンタ値とからなるエントリから、カウンタ値がしきい値を超えているものを取り出し、URLブラックリスト記憶部112に保存する。

【0102】

図12は本発明のさらに別の実施例によるメールフィルタリング装置の動作を示すフローチャートである。これら図11及び図12を参照して本発明のさらに別の実施例によるメールフィルタリング装置の動作について説明する。

【0103】

メール受信装置1はパケット情報及び電子メールの本文を取り出し、SPAM処理装置9に転送する(図12ステップS41)。SPAM処理装置9は、まず最初にURL取得手段91によって電子メールの本文に含まれる“http”から始まる文字列をURLとして取得する(図12ステップS42)。

【0104】

URL取得手段91は電子メールの本文中にURLが含まれていなかった場合(図12ステップS43)、その電子メールを第2の検索手段93に渡し、第2の検索手段93の処理を行う(図12ステップS49)。

【0105】

また、URL取得手段91はメール本文中にURLに含まれていた場合(図12ステッ

PS43)、その電子メールを第1の検索手段92に渡す。第1の検索手段92は取得URLをキーとしたエントリがメール流量記憶部101に含まれていないかどうかの検索を行う(図12ステップS44)。

【0106】

第1の検索手段92はメール流量記憶部101に抽出したURLをキーとするエントリが記憶されていた場合(図12ステップS45)、それに対応するカウンタ値を取り出して規定値だけ増加させる(図12ステップS46)。

【0107】

第1の検索手段92はメール流量記憶部101に抽出したURLをキーとするエントリが記憶されていなかった場合(図12ステップS45)、取得したURLとカウンタの初期値とからなるエントリをメール流量記憶部101に新規エントリとして保存する(図12ステップS48)。

【0108】

第1の検索手段92は規定値だけ増加させたカウンタ値がしきい値を超えていた場合(図10ステップS47)、その電子メールを迷惑メールとみなして迷惑メール処理手段94に渡すので、迷惑メール処理手段94はSPAM判定ワード記憶部102のエントリ追加処理を行う(図12ステップS51)。

【0109】

第1の検索手段92は規定値だけ増加させたカウンタ値がしきい値を超えていなければ、その電子メールを第2の検索手段93に渡す。第2の検索手段93はコンテンツのチェックを行い(図12ステップS49)、SPAM判定ワードが見つかれば(図12ステップS50)、その電子メールを迷惑メールとみなして迷惑メール処理手段94に渡すので、迷惑メール処理手段94はSPAM判定ワード記憶部102のエントリ追加処理を行う(図12ステップS51)。

【0110】

この後、迷惑メール処理手段94はSPAM判定ワード記憶部102のエントリ追加処理を行った電子メールに対して迷惑メール処理を行い(図12ステップS52)、その電子メールをメール転送装置5に渡す。メール転送装置5は迷惑メール処理手段94もしくは第2の検索手段93から送られてきたメール情報をIPパケットの形式に変換し、電子メールの送信先へと転送する(図12ステップS53)。

【0111】

ブラックリスト抽出手段111はメール流量記憶部101に保存されているURLリストからカウンタ値が閾値を超えているもののみを取り出し、URLブラックリスト記憶部112に保存する。

【0112】

本発明の一実施例では、電子メールの本文に含まれたURLを抽出してしきい値をとるので、同一サイトから大量に送られた迷惑メールを検出することができるが、複数のサイトから同一業者の広告メールが同時に送られた場合で、かつ各サイトから送られるメールの流量が閾値を下回る場合には迷惑メールとして検出されない。本実施例を用いると、それらのメールも迷惑メールとして検出することができるという新たな効果を奏する。

【図面の簡単な説明】

【0113】

【図1】本発明の一実施例によるメールフィルタリング装置の構成を示すブロック図である。

【図2】本発明の一実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【図3】本発明の一実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【図4】本発明の一実施例においてSPAM判定ワード記憶部に登録して迷惑メールのチェックを行う理由を示す図である。

【図5】本発明の他の実施例によるメールフィルタリング装置の構成を示すブロック図である。

【図6】本発明の他の実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【図7】本発明の他の実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【図8】本発明の別の実施例によるメールフィルタリング装置の構成を示すブロック図である。

【図9】本発明の別の実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【図10】本発明の別の実施例によるオペレータ制御部における登録候補リスト選択処理を示すフローチャートである。

【図11】本発明のさらに別の実施例によるメールフィルタリング装置の構成を示すブロック図である。

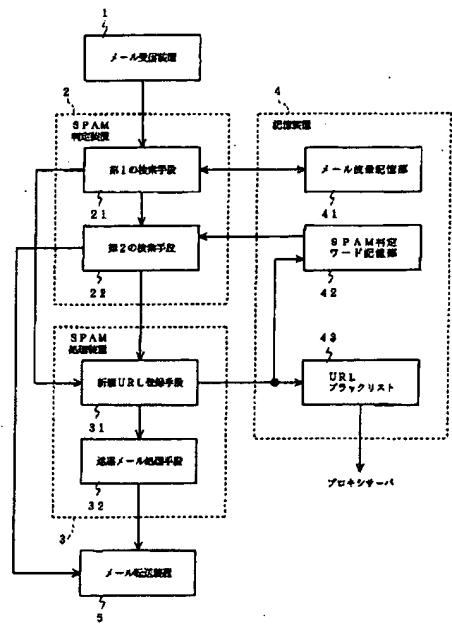
【図12】本発明のさらに別の実施例によるメールフィルタリング装置の動作を示すフローチャートである。

【符号の説明】

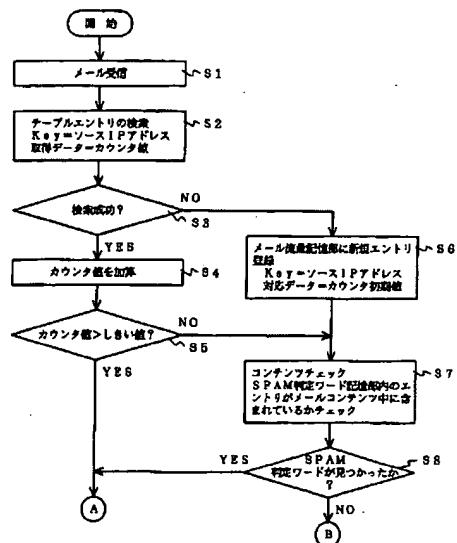
【0114】

- 1 メール受信装置
- 2 SPAM判定装置
- 3, 9 SPAM処理装置
- 4, 6, 7, 10 記憶装置
- 5 メール転送装置
- 8 オペレータ制御部
- 11 ブラックリスト構築装置
- 21, 92 第1の検索手段
- 22, 93 第2の検索手段
- 31 新規URL登録手段
- 32, 94 迷惑メール処理手段
- 41, 101 メール流量記憶部
- 42, 102 SPAM判定ワード記憶部
- 43 URLブラックリスト
- 61 URLホワイトリスト
- 71 登録候補リスト
- 91 URL取得手段
- 111 ブラックリスト抽出手段
- 112 URLブラックリスト記憶部

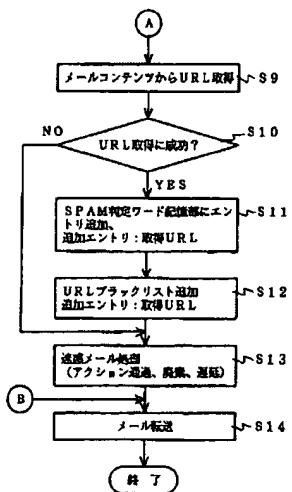
【図1】



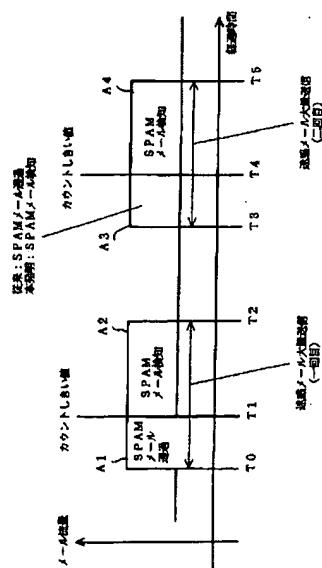
【図2】



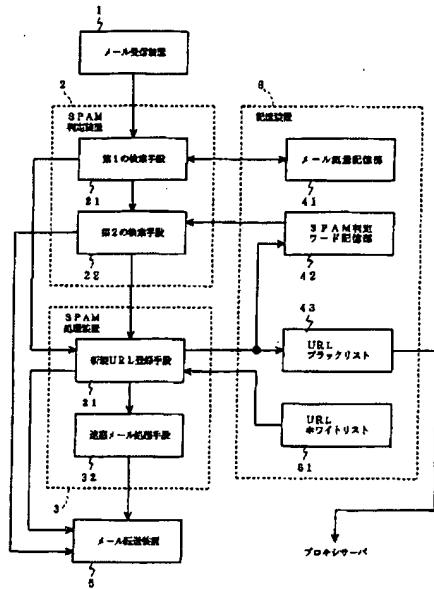
【図3】



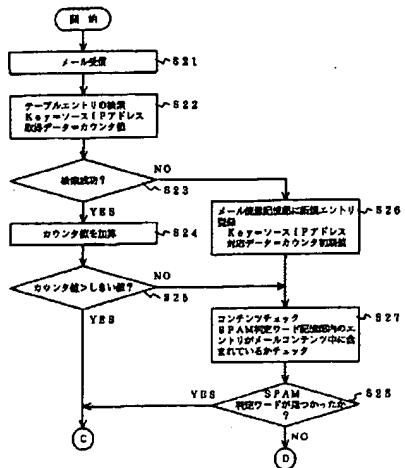
【図4】



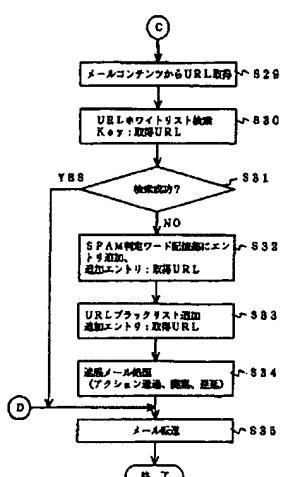
【図5】



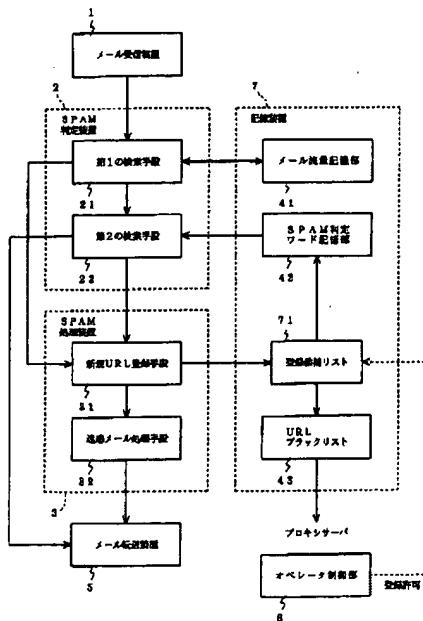
【図6】



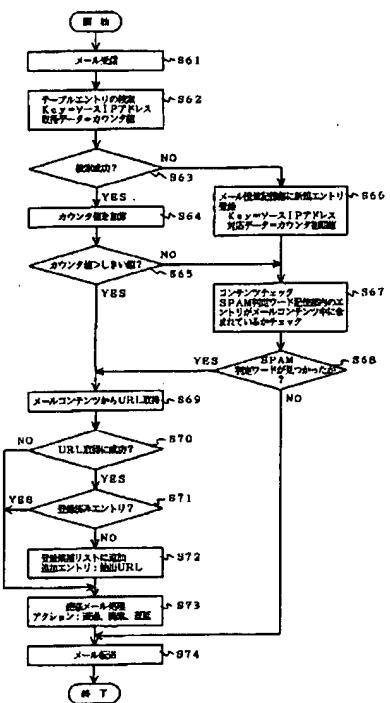
【四7】



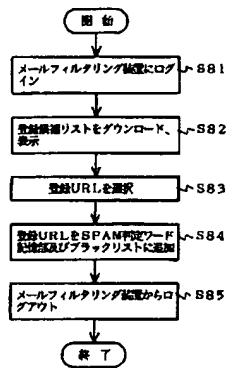
【図8】



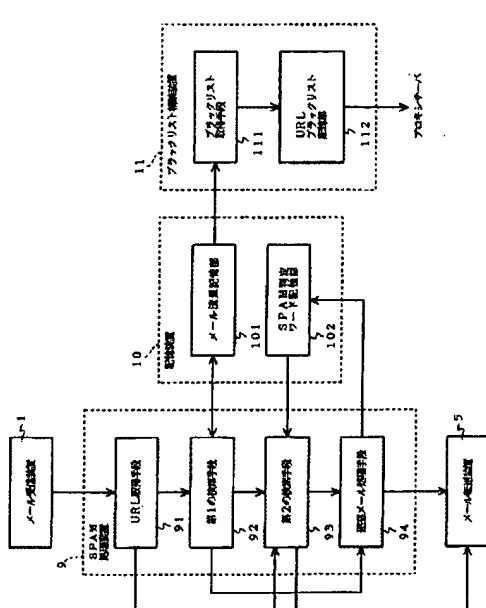
【図9】



【図10】



【习题11】



【図12】

